Interação entre usuários, tecnologia e sistema informatizado de gestão arquivística de documentos: percepções teóricas

Interaction between users, technology, and computerized document archival management system: theoretical insights

Ana Paula Monteiro Almeida Chagas
Mestra em Ciência da Informação pela Universidade Federal de Sergipe, UFS, São Cristóvão, SE, Brasil;
ORCID: https://orcid.org/0009-0008-1813-699X
E-mail: anapaulamonteiroac@gmail.com

Telma de Carvalho
Doutora em Ciência da Informação pela Universidade de São Paulo; Professora do Programa de Pós-Graduação em Ciência da Informação pela Universidade Federal de Sergipe, UFS, São Cristóvão, SE, Brasil;
ORCID: https://orcid.org/0000-0001-8700-2452
E-mail: telmac@academico.ufs.br

Resumo

Inserida no contexto das transformações proporcionadas pelas Tecnologias da Informação e Comunicação (TIC), com a influência direta da Internet e a disseminação dos sistemas de informação informatizados, que marcaram a Era da Informação, esta pesquisa de revisão bibliográfica teve como propósito analisar as principais perspectivas teóricas encontradas na literatura científica sobre o comportamento dos usuários em relação à segurança da informação no uso de Sistemas Informatizados de Gestão Arquivística de Documentos (Sigad), considerando a interface entre usuários, máquinas e sistemas. Explorou-se a relevância desses sistemas, bem como os riscos e vulnerabilidades a que estão sujeitos, enfatizando o papel dos usuários e a temática da segurança da informação no âmbito da Ciência da Informação (CI) e seus fenômenos correlatos. No decorrer das análises, constatou-se que tanto a ausência de uma política de segurança da informação implementada de maneira colaborativa, democrática e acessível, envolvendo tanto gestores quanto colaboradores, como a falta de conscientização dos usuários como participantes ativos nas iniciativas de segurança da informação, podem constituir pontos críticos para a segurança das informações. Conclui-se, portanto, que subsiste uma lacuna substancial na abordagem atual da segurança da informação, particularmente no que concerne à interface entre o ser humano, a máquina e o sistema. Para assegurar a efetividade e a integridade das medidas de segurança, torna-se imprescindível aprofundar a análise e a discussão dessas vulnerabilidades, visando fortalecer o entendimento desse tema de maneira abrangente. A análise dos estudos mostrou uma maior incidência na área da CI, com correlações entre essa área, a Ciência dos Dados e a Ciência da Computação. Os aspectos socioculturais também ganharam relevância, incluindo abordagens voltadas para o estudo dos usuários e suas interações com o homem, tecnologia e sistema.

Palavras-chave: comportamento de usuários; segurança da informação; sistema informatizado de gestão arquivística de documentos; sistemas de informação.

Abstract

Inserted in the context of the transformations brought about by information and communication technologies under the direct influence of the internet and the dissemination of computerized information systems, which marks the Information Age, this bibliographic review research aimed to analyze the main perspectives theoretical findings in the scientific literature on user behavior concerning information security when using computerized document archival management systems, considering the interface between users, machines, and systems. The relevance of these systems and the risks and vulnerabilities to which they are subject were explored, emphasizing the role of users and the issue of information security within the scope of information science and its related phenomena. The analysis showed that the absence of an information security policy implemented in a collaborative, democratic, and accessible manner involving both managers and employees and the lack of awareness among users as active participants in information security initiatives may constitute critical points for information security. Therefore, there remains a substantial gap in the current approach to information security, particularly about the interface between the human beings, machines, and systems. Ensuring the effectiveness and integrity of security measures must further develop the analysis and discussion of these vulnerabilities to strengthen the understanding of this topic in a comprehensive manner. The analysis of the chosen articles showed a higher incidence in information science, with correlations between this area and data science and computer science. Sociocultural aspects also gained relevance, including approaches focused on studying users and their interactions with people, technology, and systems.

Keywords: user behavior; information security; computerized document archival management system; information systems.

1. Introdução

O mundo globalizado foi profundamente impactado por uma aventura humana e tecnológica que transcendeu as limitações de tempo e espaço, gerando alterações substanciais nos processos socioculturais, econômicos e políticos em toda a sociedade. Essa evolução introduziu novas formas de acesso, tratamento, recuperação, compartilhamento e disseminação da informação, abrindo um vasto leque de possibilidades e transformando a informação em um recurso estratégico de elevada importância para a tomada de decisões e a construção do conhecimento. Essas mudanças vieram coroar a Era da Informação.

A informação adquiriu um status decisório para conduzir os processos gerenciais e administrativos nas organizações. O seu valor ganhou *know-how* em alicerçar a Gestão da Informação (GI) e a Gestão do Conhecimento (GC), sendo esse também o seu grande desafio: gerir os fluxos informacionais produzidos em alta escala (Almeida; Biaggi; Vitoriano, 2021).

É relevante salientar que, respaldados pelas Tecnologias da Informação e da Comunicação (TIC) e pela Internet, os sistemas informatizados de informação emergem com o propósito de aprimorar a GI ao longo do ciclo de vida dos documentos. Andrade e Valentim (2019) enfatizam a necessidade da interação entre a GI e a GC como fundamental para impulsionar essas transformações, as quais têm um impacto positivo nos processos gerenciais, baseados no fluxo informacional, e oferecem suporte para a efetiva implementação dessas mudanças.

A automação desses sistemas possibilitou integrar as práticas de GI com os processos gerenciais para fins de otimizar os produtos e serviços prestados pela organização. Contudo, a implementação de um sistema de informação envolve diferentes elementos que interagem entre si, reconhecidos nesta pesquisa como a interface homem, máquina e sistema.

Destaca-se o Sistema Informatizado de Gestão Arquivística de Documentos (Sigad), o qual tem funcionalidades para gerir o ciclo de vida dos documentos digitais e eletrônicos, com capacidade para gerenciar grandes volumes de informação em suporte digital.

Nessa perspectiva, considerando que o fluxo informacional nos sistemas de informação é simultaneamente acessado por diferentes usuários de forma remota, ultrapassando as barreiras de tempo e espaço e a iminência de ataques cibernéticos, que têm provocado prejuízos

incalculáveis para as organizações, o tema segurança da informação tem crescido em razão da necessidade de sua gestão para conscientização de boas práticas pelos usuários.

A convergência digital já vinha transformando o uso de sistemas informacionais e as atividades laborais, principalmente nos últimos dois anos, período pandêmico da Covid-19, em que prevaleceu a modalidade de trabalho remoto e no período pós-pandêmico, no qual foi instituída essa modalidade de trabalho por algumas organizações, principalmente governamentais. Sob essa ótica, surge a necessidade de se desenvolver uma política de segurança da informação, seja na concepção tecnológica, de usuários ou dos sistemas, cada vez mais expostos a vulnerabilidades e riscos.

Nesse contexto, justificado pela importância da segurança da informação no âmbito da CI e os fenômenos que dela emergem, esse estudo objetivou analisar na literatura científica as principais percepções teóricas sobre o comportamento dos usuários em segurança da informação no uso de um Sigad na concepção da interface homem, máquina e sistemas.

2. A relevância da informação na era da informação

Situar a informação nessa conjuntura é salutar para a área da CI, porque ela fomenta todos os fenômenos de transformação socioculturais que promoveram as mudanças paradigmáticas na Sociedade da Informação.

Valentim (2008) enfatiza que a informação é um insumo essencial para todos os processos que agregam valor aos negócios. Essa importância se estende além de sua função na construção do conhecimento, abrangendo também a vasta expansão facilitada pelas tecnologias. Para a autora, essas tecnologias oferecem as ferramentas necessárias para acessar, armazenar, processar e compartilhar informações, culminando na geração de conhecimento como o desfecho final desse processo.

Silva (2017) argumenta que a informação é composta por componentes valorativos, os quais estão intimamente relacionados com as práticas informacionais. Essas práticas determinam a importância do seu uso, estabelecendo uma inter-relação que pode ser causal ou consequencial. A autora argumenta que o valor da informação é determinado pela circunstância em que é usada, incluindo fatores humanos, sociais, culturais, religiosos, científicos e econômicos. Embora os valores consequenciais, como produtividade e comércio, sejam mais

reconhecidos, o processo de atribuição de valor à informação é um campo subexplorado que precisa de mais atenção.

No campo organizacional e da produtividade, Santos e Valentim (2020) ampliam o conceito da informação como eixo para a competitividade, podendo a ela ser atribuído um valor econômico resultante do seu processo final de gerar produtos competitivos. Destacam a sua importância nos processos decisórios, pela capacidade de sinalizar os erros e acertos para a tomada de decisão, podendo dessa forma reduzir incertezas e contribuir para a inovação e vantagem competitiva nas organizações (Santos; Valentim, 2020).

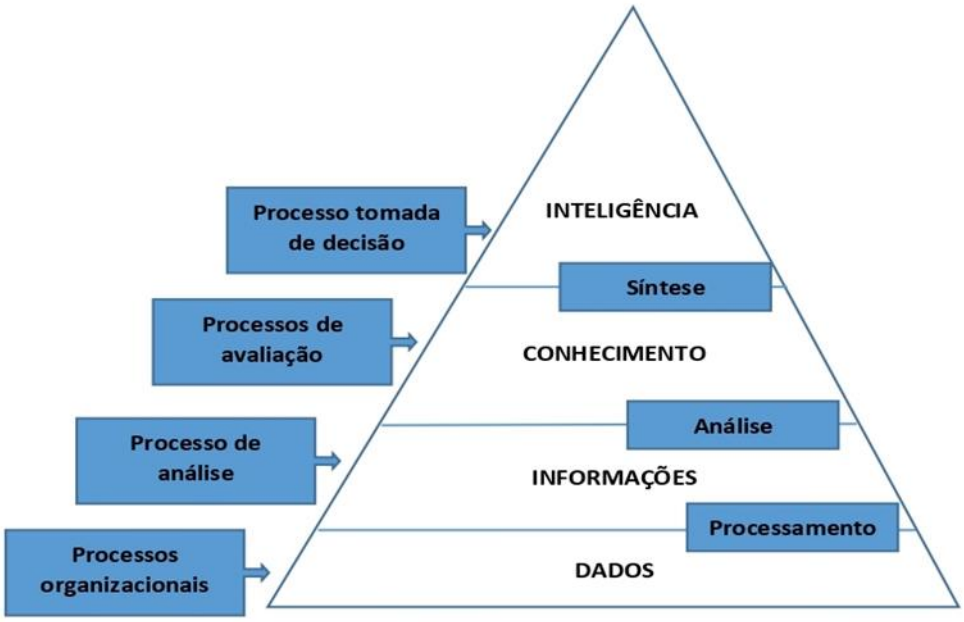
Para Teixeira e Valentim (2015) a informação parte de elementos objetivos e subjetivos, cujo significado é atribuído por um sujeito cognoscente com capacidade de apropriação, podendo gerar o conhecimento organizacional que se renova a cada novo ciclo informacional.

Relacionando a gestão efetiva de uma organização com a percepção objetiva do valor que a informação pode agregar, Moresi (2000) entende que o principal valor da informação está relacionado aos seus fatores estruturais e instrumentais, que influenciam diretamente a gestão decisória e as ações estratégicas na tomada de decisão. Como ponto crítico em qualquer sistema de informação, o autor destaca os fatores de disponibilidade e acesso à informação para uso estratégico.

Choo (2003) enfatiza que a capacidade cognitiva dos usuários é fundamental na atribuição de significados à informação, ampliando significativamente seu valor. Esse valor está essencialmente ligado à forma como os usuários utilizam a informação e percebem sua capacidade de atender às necessidades e resolver demandas específicas. Em outras palavras, o seu valor é construído por meio da habilidade dos usuários em contextualizá-la para satisfazer suas necessidades e resolver problemas de maneira eficaz.

Em conformidade com Urdaneta (1992), a cadeia que abrange a valorização, produção e disseminação da informação é estruturada hierarquicamente em quatro categorias essenciais: dados, informação, conhecimento e inteligência. Essas categorias são interdependentes e apresentam atributos tanto qualitativos quanto quantitativos. Essa hierarquia oferece uma visão sistemática de como a informação evolui e se transforma, desde sua origem como dados brutos, até sua aplicação como inteligência na tomada de decisões, como ilustrado na Figura 1.

Figura 1 – Dados sobre a circulação de determinado local em determinado período de tempo



Fonte: Adaptado de Urdaneta (1992).

Conforme os níveis de informação mencionados acima, Urdaneta (1992) estabelece uma relação fundamental entre o ciclo de produção e transferência de informações e os estágios de processamento, análise e síntese da informação, que contribuem para a criação de valor. A representação mostra que os principais componentes que constituem o modelo estão intensamente interligados e são distribuídos entre as diversas categorias no diagrama.

Nessa configuração, os dados se destacam, servindo como componentes quantitativos pelos quais a informação é introduzida no sistema. Originados de várias fontes, esses dados constituem a matéria-prima inicial do processo. A autora demonstra que a avaliação qualitativa das diferentes categorias hierárquicas de informação inicia-se com o processo de análise, no qual "o estado do conhecimento ocorre quando estamos em condições de interpretar completamente o significado da informação" (Urdaneta, 1992, p. 111).

Por fim, na conclusão do diagrama mencionado, a evolução do conhecimento se completa na fase da inteligência, essencial na tomada de decisões. Essa etapa é considerada a mais qualitativa e significativa na hierarquia, pois depende da experiência humana e da inteligência inerente à organização e à gestão.

Em consonância com Urdaneta (1992), autores renomados, como Davenport e Prusak (1999), ressaltam a relação inseparável entre dados, informação e conhecimento, indicando que esses três elementos são interdependentes e interligados. Essa sequência, alinhada com a visão

dos autores, ilustra a transformação contínua e o aumento de valor desses elementos na cadeia de informação e conhecimento. O desafio central reside em reconhecer o conhecimento como um ativo corporativo, isto é, dar a devida importância à sua gestão e proteção, equiparando-o em termos de valor aos ativos mais tangíveis da organização, ou seja: "geri-lo, cercá-lo do mesmo cuidado dedicado à obtenção de valor de outros ativos mais tangíveis" (Davenport; Prusak, 1999, p. 14).

É possível afirmar que, com base na cadeia de valor da informação, esse ciclo contínuo e retroalimentado está estrategicamente alinhado com o propósito de maximizar o valor da informação, assegurando que ele seja constantemente incorporado ao longo do ciclo informacional, com o intuito de sua aplicação estratégica.

2.1 Sistemas informatizados de gestão arquivística de documentos (Sigad)

A transformação digital conferiu à informação um protagonismo nos processos informacionais. Nesse sentido, Jadertrierveiler, Sell e Santos (2019) atribuem essa mudança como decorrente do movimento da conectividade global, que impulsionou a evolução da infraestrutura tecnológica, culminando com a intensificação desse processo a partir do ano 2000, marcando o início da Era Digital.

Os autores citados creditam às tecnologias de informação as transformações na estrutura funcional e tecnológica dos ambientes organizacionais, conferindo-lhes dinamismo e complexidade. Essas novas ferramentas possibilitaram a gestão eficaz de volumes significativos de dados, além da capacidade de gerar informações e promover a criação de conhecimento organizacional (Jadertrierveiler; Sell; Santos, 2019).

Castells (2013) identifica uma realidade virtual tangível e substancial que demanda a adoção de novas práticas em sintonia com os avanços tecnológicos e sociais em uma economia, cultura e sociedade inteiramente interconectadas em rede. Essa nova realidade representa um desafio e uma oportunidade significativos para a forma como interagimos e operamos em um mundo cada vez mais digitalizado. Para o autor, "A globalização também modifica os mercados de trabalho e posiciona o multiculturalismo na vanguarda da dinâmica social" (Castells, 2013, p. 12).

É possível estabelecer um paralelo entre o avanço tecnológico e a incorporação da informação em novos formatos nos sistemas informatizados, o que tornou a gestão documental mais complexa e desafiadora, abrangendo desde a produção até a autenticidade e recuperação dos documentos digitais. Silva e Rocha (2022) argumentam que os documentos digitais com funções jurídicas ou administrativas passaram a coexistir e depender dos sistemas informatizados, os quais, por sua vez, devem atender a um padrão de funcionalidade que permita a manutenção da gestão dos processos do trabalho.

Baseado em Moresi (2000), o sistema de informação é um elemento-chave na representação eficiente e disseminação da informação, contribuindo significativamente para a sua cadeia de valor e para o processo de geração de conhecimento nas organizações. Em sua visão, ao longo do ciclo de vida da informação, os sistemas informatizados têm a capacidade de aprimorar essa representação e disseminação. Moresi (2000, p. 23) assim define um sistema de informação: "É uma combinação de processos relacionados ao ciclo informacional, de pessoas e de uma plataforma de tecnologia da informação, organizados para o alcance dos objetivos de uma organização".

Visando lidar com o considerável volume de informações geradas e recebidas durante as atividades e processos de trabalho das organizações, os sistemas informatizados surgiram como um apoio fundamental para a gestão de documentos digitais. Baseado nas orientações da Câmara Técnica de Documentos (CTDE) do Conselho Nacional de Arquivos (Conarq [2020]), a administração adequada de documentos digitais deve ser realizada por meio de um Sigad.

Baseado no Conarq (2020), o Sigad tem maior controle da gestão do ciclo de vida dos documentos se comparado ao Gerenciamento Eletrônico de Documentos (GED) e à Enterprise Content Management (ECM). Esses últimos sistemas, embora desempenhem funções de gerenciamento de documentos, nem sempre incorporam uma hermenêutica arquivística, como detalhado a seguir:

> Um GED ou um ECM tratam os documentos de maneira compartimentada, enquanto o Sigad parte de uma concepção orgânica, qual seja, a de que os documentos possuem uma inter-relação que reflete as atividades da instituição que os criou. Além disso, diferentemente do Sigad, o GED ou o ECM nem sempre incorporam o conceito arquivístico de ciclo de vida dos documentos (Conarq, 2020, p. 28).

Dado o incremento de segurança proporcionado pela gestão documental em sistemas informatizados, bem como o controle mais eficiente do ciclo de vida dos documentos, o Conarq apresenta a seguinte definição para o Sigad:

> Solução informatizada que visa o controle do ciclo de vida dos documentos, desde a produção até a destinação final, seguindo os princípios da gestão arquivística de documentos. Pode compreender um software particular ou um determinado número de softwares integrados, adquiridos ou desenvolvidos por encomenda (Conarq, 2020, p. 27).

Segundo a Câmara Técnica de Documentos Eletrônicos (CTDE) do Conarq (2020), o Sigad tem a funcionalidade de gerenciar a elevada produção de documentos produzidos de forma eletrônica, digital ou híbrida de forma confiável. Isso inclui operações de captura, armazenamento, acesso a documentos, aplicação de plano de classificação, controle de prazos de retenção e destinação, bem como a preservação a médio e longo prazo de documentos arquivísticos, sejam eles digitais ou não, até seu destino final.

Com base na Orientação Técnica nº 1, de abril de 2011, a CTDE fornece diretrizes essenciais para a aquisição de um Sigad, abordando os seguintes aspectos: o controle abrangente do ciclo de vida dos documentos, a escolha entre a utilização de um único software ou a integração de múltiplos sistemas, e a gestão de documentos em formatos digitais, convencionais e híbridos. O conjunto de requisitos essenciais para um Sigad foi cuidadosamente delineado com base nas diretrizes normativas e conceituais da gestão de documentos.

De acordo com os requisitos do Sigad, são estabelecidos padrões que devem ser seguidos ao longo do ciclo de vida do documento na organização. Esses padrões promovem boas práticas de segurança da informação e eficiência na gestão de documentos eletrônicos. Esses requisitos incluem objetivos e planos de ação definidos para garantir uma gestão documental eficaz que abranja processos e sistemas.

O e-ARQ Brasil, um Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos, lançado em 2006, passou por várias atualizações para se manter alinhado com as inovações tecnológicas. A Comissão Técnica de Documentos Eletrônicos (CTDE) supervisiona sua implementação em várias organizações (Conarq, 2020). O Sigad tem como base documentos arquivísticos e requer a implantação prévia de um programa de gestão arquivística, abrangendo diversos formatos documentais (Conarq, 2020).

Vendramini e Aleixo (2021) destacam a complexidade da gestão de documentos produzidos em formato digital, especialmente no que diz respeito ao cumprimento dos requisitos arquivísticos. Elas argumentam que os principais modelos de requisitos estabelecidos pelo Sigad têm sua base no conceito do ciclo vital dos documentos, que é fundamental para a Gestão Documental (GD).

Contudo, ao efetuarem uma análise das 44 seções de requisitos contidas nos 14 capítulos do Sigad desenvolvido pelo e-ARQ Brasil (Conarq, 2020), as autoras identificaram que aproximadamente um terço dessas seções estrita e rigorosamente se alinha com os princípios basilares das práticas arquivísticas. Por outro viés, as duas partes remanescentes desses requisitos estão alicerçadas em conhecimentos direcionados para as especificidades inerentes ao próprio sistema em questão.

Costa (2018) argumenta que o considerável número de seções direcionadas às particularidades do Sigad é justificado pela relevância da arquivística como integrante do sistema. Isso ocorre porque a arquivística está associada ao gerenciamento do Sigad, fornecendo o arcabouço teórico e prático para sua implementação. Ao integrar os princípios e normas arquivísticas, o sistema é moldado para atender às necessidades dos usuários de forma precisa e completa.

Além disso, Costa (2018) afirma que a modelagem do Sigad estabelece uma relação intrínseca entre os princípios fundamentais dos documentos arquivísticos e os diversos tipos de documentos, sejam eles de natureza nato-digital, digital, digitalizada ou física, sem levar em consideração o meio de armazenamento. Partindo dessa compreensão, o autor chega à seguinte conclusão: “O Sigad está preparado para todas as possibilidades de trabalho a ser desenvolvido tendo como fonte informativa o documento de arquivo” (p. 102).

É relevante destacar que, no que tange os profissionais da informação, os desafios são uma constante, assim como a contínua evolução dos sistemas de informação. Para Alencar e Araújo Júnior (2022), a experiência prática obtida por meio da implementação e uso de sistemas informatizados em um ambiente organizacional frequentemente revela áreas que podem ser otimizadas ou ajustadas para melhorar a eficiência e eficácia desses sistemas. Esse processo está estreitamente relacionado ao estudo dos usuários e às suas necessidades informacionais, concluem os autores.

Em continuidade às análises de Alencar e Araújo Júnior (2022), durante o planejamento de implementação de um Sigad é comum ocorrer a falta de devida investigação das necessidades informacionais dos usuários, assim como a ausência de avaliação das principais dificuldades que enfrentam nos processos de recuperação da informação. Para os autores, essas constatações têm o potencial de desencadear a necessidade de realizar revisões nos requisitos do sistema, com o objetivo de promover um alinhamento mais eficaz do Sigad com as metas e objetivos da organização. Isso implica em manter os sistemas atualizados e alinhados com as

novas demandas, incluindo a incorporação de inovações que possam melhorar a eficiência operacional (Alencar; Araújo Júnior, 2022).

A evolução dos sistemas informatizados tem implicações significativas em uma variedade de contextos organizacionais. Santos e Flores (2018) identificam que os sistemas informatizados criaram novos rumos para a preservação dos documentos digitais, expandindo o conceito dos documentos e a eles atribuindo uma série de ações e reflexões que vieram influenciar a revisão e a necessidade de possíveis ajustes nos requisitos dos Sigad ao longo do tempo. Em resumo, pode-se compreender que acompanhar a evolução dos sistemas e revisar requisitos de forma proativa garantem que essas ferramentas continuem a contribuir eficazmente para as operações e processos organizacionais.

2.2 Comportamento dos usuários na perspectiva de segurança da informação

Em nível organizacional, geralmente a segurança da informação está voltada para maiores investimentos em questões tecnológicas, algumas vezes negligenciando o fator humano. Sob esse enfoque, Dhillon (2004) argumenta que os pilares da segurança da informação são fundamentados nas pessoas, tecnologia e sistemas, em que a própria definição de segurança da informação está fundida a elementos que envolvem a interação de pessoas com o uso dos sistemas, sendo eles: a confidencialidade, a integridade, a responsabilidade, a honestidade das pessoas, a confiança e a ética.

Sêmola (2003) apresenta uma definição ampla e voltada para questões mais subjetivas de segurança da informação que avança os princípios tecnológicos e se respalda em questões estruturais comportamentais. Ele define a segurança da informação como: “Área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade” (Sêmola, 2003, p. 41).

Furnell e Thomson (2009) advogam que são estreitas as relações que desencadeiam os riscos à segurança da informação, que predominantemente envolvem pessoas e tecnologia. Os autores descrevem atitudes apáticas, desinteresse, negligência e ações descomprometidas com a proteção dos ativos informacionais como riscos prevalecentes por parte dos usuários do sistema. Os autores supracitados sugerem o desenvolvimento de uma cultura corporativa moldada para a conscientização e instrução dos funcionários como forma de garantir o desenvolvimento e habilidades relevantes e voltadas para segurança da informação.

Ferreira (2017) destaca a importância da política de segurança da informação e a necessidade de conscientização dos usuários sobre seu papel nas questões relacionadas a essa área. O autor enfatiza que os riscos de segurança podem emergir da falta de conformidade dos usuários com as políticas e princípios fundamentais de segurança da informação.

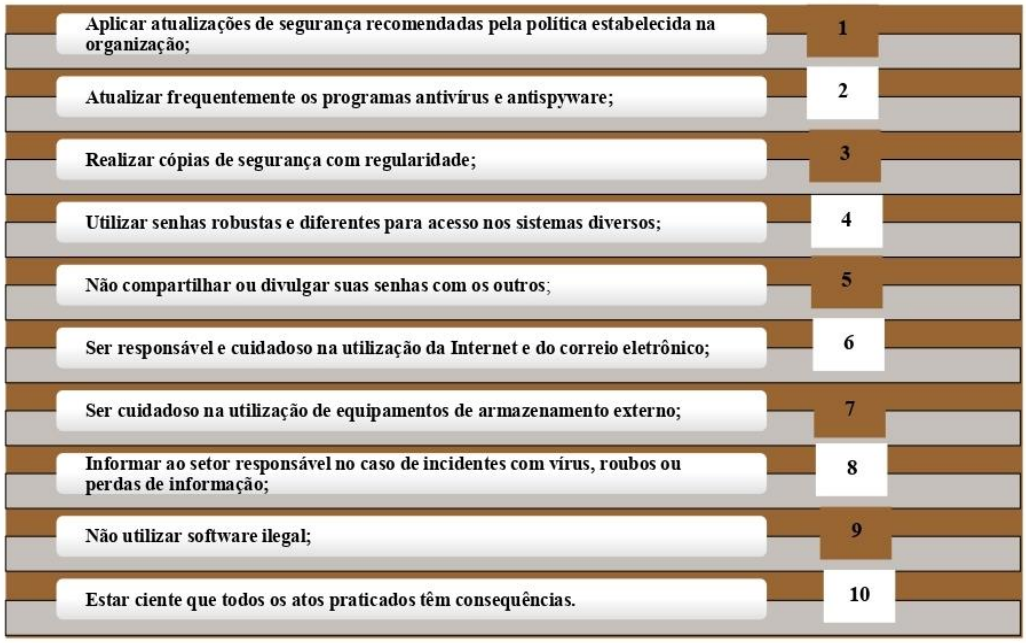
Essa análise sublinha que a eficácia das políticas de segurança não depende apenas da implementação de medidas técnicas, mas também da adesão e compreensão dos usuários. A conscientização contínua e a educação sobre práticas de segurança são fundamentais para mitigar riscos e proteger as informações, pois os usuários desempenham um papel ativo na segurança organizacional e podem ser a linha de defesa contra ameaças cibernéticas.

A observação feita por Ferreira (2017) é particularmente relevante, uma vez que os riscos de segurança da informação frequentemente começam com pequenas negligências do usuário, como a abertura de anexos suspeitos e de *links* maliciosos em e-mails. Embora essas ações possam parecer inofensivas, elas representam pontos de entrada para potenciais ameaças cibernéticas.

Ferreira (2017) argumenta ainda que essas práticas descuidadas podem evoluir para ataques significativos aos bancos de dados que armazenam informações sensíveis e críticas, resultando em consequências prejudiciais para a organização, como vazamento de dados, perda financeira e danos à reputação. Esses ataques podem ser realizados por *hackers* mal-intencionados que exploram vulnerabilidades no sistema de segurança da informação. Além disso, a falta de conscientização e treinamento adequado dos funcionários pode agravar ainda mais a situação, tornando a organização um alvo fácil para cybercriminosos.

Consoante com a compreensão do autor, a Figura 2 apresenta as dez principais medidas de boas práticas essenciais para a segurança da informação.

Figura 2 – Principais mecanismos de boas práticas de segurança da informação



Fonte: Adaptado de Ferreira (2017, p. 88-89).

No âmbito das boas práticas em segurança da informação, Ferreira (2017) ainda destaca a importância de incorporar uma estratégia colaborativa à política de segurança da informação, na qual são considerados os problemas e vulnerabilidades percebidos pelos usuários dos sistemas. Isso se torna particularmente relevante diante do aumento alarmante dos índices de violações e ataques cibernéticos. O autor sustenta que a elaboração de mecanismos de defesa capazes de identificar ameaças e reduzir a vulnerabilidade dos sistemas se destaca como a estratégia mais eficaz para a gestão da segurança da informação.

Hitchings (1995) identifica uma lacuna significativa na pesquisa relacionada aos usuários de Sistemas de Informação (SI), especificamente no que diz respeito à sua participação efetiva no planejamento e controle das políticas de segurança da informação dentro das organizações. O autor conclui que essa carência limita a capacidade de implementar mudanças que poderiam oferecer contribuições colaborativas para aprimorar as políticas de segurança da informação e também restringe a identificação precisa dos problemas reais enfrentados pelos usuários nesse cenário.

Marciano (2006) critica a abordagem tradicional das políticas de informação, que frequentemente se limita a códigos de conduta impostos aos usuários. Para o autor, essa conduta é pouco eficaz em promover uma cultura de segurança da informação, uma vez que não engaja os usuários de forma significativa. Em contrapartida, Marciano defende uma ideia mais proativa, que eleve os usuários a agentes ativos na gestão da informação, participando

ativamente na construção e implementação das políticas, fundamental para garantir a sua efetividade.

Observando-se os mecanismos relativos à defesa para as boas práticas de segurança da informação discutidos no *corpus* dessa seção, pode-se vislumbrar que as ações sugeridas são pertinentes para prevenção de eventuais danos aos SI e à vulnerabilidade do seu uso. Essas ações visam prevenir as vulnerabilidades e eventuais danos nos sistemas de informação pela falta de sensibilidade e consciência no uso das práticas corretas para o desempenho das suas atividades laborais na organização.

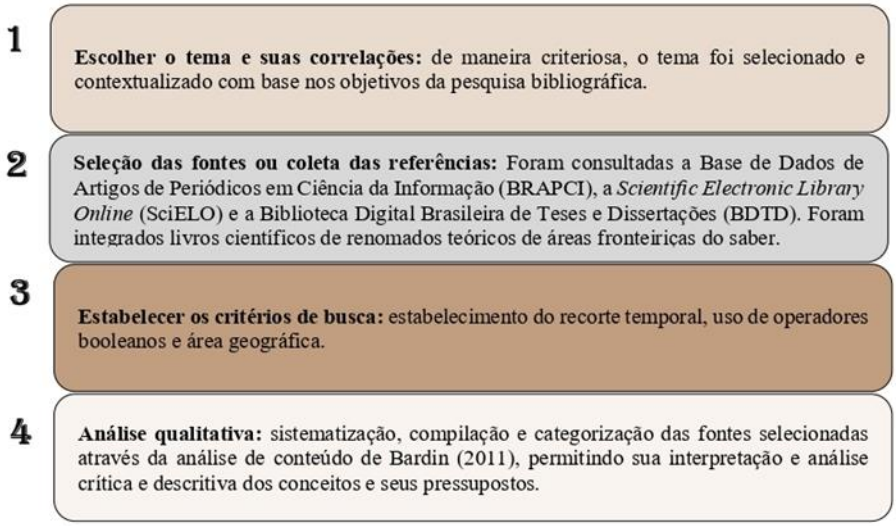
3. Metodologia

Neste estudo, utilizou-se uma pesquisa com abordagem qualitativa e cunho descritivo, aprofundando-se teoricamente com uma pesquisa de revisão bibliográfica voltada para as percepções teóricas que inter-relacionam os usuários de sistemas, a tecnologia e os Sigad. Para a coleta de dados, de acordo com o item 2 do checklist (Figura 2), foram selecionadas a Base de Dados em Ciência da Informação (Brapci), a *Scientific Electronic Library Online* (Scielo) e o Portal de Periódicos CAPES. A busca foi ampliada na Biblioteca Digital Brasileira de Teses e Dissertações (BDTD) e em fontes bibliográficas de referência na área, buscando ampliar o escopo da pesquisa e acessar um conjunto diversificado de trabalhos acadêmicos.

A escolha pela revisão narrativa de literatura se justifica porque esse método, embora com natureza teórica, quando estabelecido critérios de busca criteriosos, proporciona uma análise ampla e crítica das fontes existentes, permitindo identificar e sintetizar o conhecimento atual sobre o tema.

Conforme enfatizam Marconi e Lakatos (2017), a identificação precisa da produção científica em uma pesquisa bibliográfica requer um planejamento meticuloso. Nessa conjuntura, as autoras delineiam oito fases para a condução eficaz da pesquisa bibliográfica: “a) escolha do tema; b) elaboração do plano de trabalho; c) identificação; d) localização; e) compilação; f) fichamento; g) análise e interpretação; h) redação” (Marconi; Lakatos, 2017, p. 59). Com base nas fases propostas pelas autoras, foi desenvolvido e adaptado um *checklist* que foi rigorosamente seguido durante a condução desta pesquisa bibliográfica (Figura 2).

Figura 3 – Checklist das etapas da pesquisa bibliográfica



Fonte: elaborado pelas autoras a partir de Marconi e Lakatos (2017).

Com abrangência de seis meses, de março a setembro de 2023, a estratégia de busca e refinamento da pesquisa foi cuidadosamente delineada, facilitando a seleção e subsequente utilização do material recuperado no estudo. Como critério de exclusão, estabeleceu-se um limite temporal de até dez anos de publicação para os artigos, teses e dissertações, com exceção dos artigos de especialistas amplamente reconhecidos na área e das publicações de livros, que não foram sujeitos a essa restrição temporal. O limite temporal foi estabelecido para garantir a relevância das pesquisas em relação ao estado da arte da área. Foi delimitado o território brasileiro para análise dos estudos.

Foram utilizados os operadores booleanos lógicos AND e NOT para aumentar a precisão e o refinamento na busca de publicações científicas, considerando como pontos de acesso os principais termos encontrados nos resumos e nas palavras-chave.

A contribuição da análise de conteúdo para a validade e confiabilidade da pesquisa, conforme defendido por Bardin (2011), reside na sua capacidade de proporcionar uma estrutura sistemática e rigorosa para a análise e interpretação dos dados. Esse método se justifica pelos seguintes motivos: “O analista, tendo à sua disposição resultados significativos e fiéis, pode então propor inferências e adiantar interpretações a propósito dos objetivos previstos – ou que digam respeito a outras descobertas inesperadas” (Bardin, 2011, p. 131).

Por meio da sua categorização foi possível organizar informações textuais complexas de maneira lógica e compreensível para conseguir identificar as principais percepções teóricas sobre usuários, segurança da informação, Sigad e suas interfaces com o homem, tecnologia e sistemas.

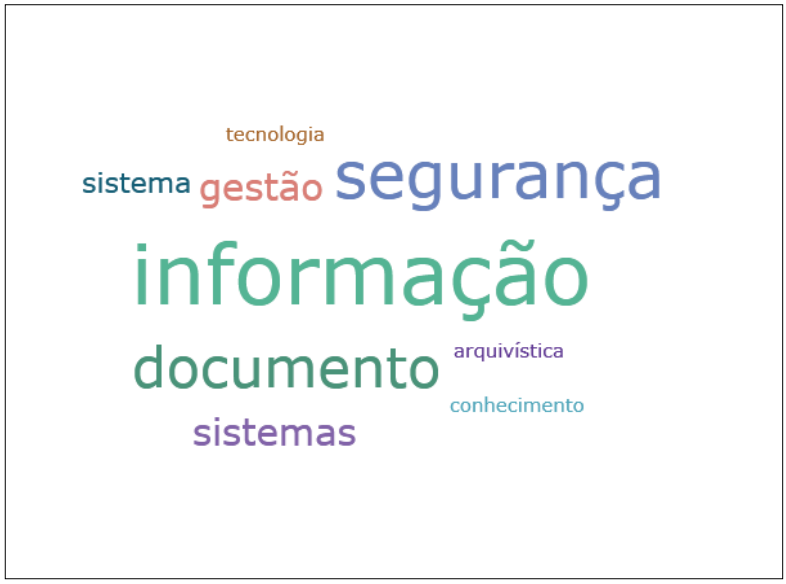
4. Resultados e discussão

Por meio da literatura sobre segurança da informação no âmbito da CI, observou-se uma inclinação predominante em direção às questões relacionadas ao valor da informação e aos processos da GI e da GC em diversas perspectivas. Os fenômenos que circundam essa temática refletem as transformações nos aspectos tecnológicos, econômicos e sociais da Sociedade da Informação, uma tendência que se conecta às questões abordadas neste estudo.

A análise categorial dos conteúdos foi estruturada em torno de três eixos principais: valor da informação e tecnologia, Sigad e Segurança da Informação, com ênfase nas interfaces homem, máquina e sistema. Essas dimensões orientaram a classificação e a análise de conteúdo do corpus da pesquisa

Na Era da Informação, observa-se uma crescente valorização dos documentos e da segurança dos sistemas. Essa tendência é evidenciada pela análise da nuvem de palavras (Figura 3), que demonstra a forte associação entre esses elementos.

Figura 4 – Nuvem de palavras: critérios, valor da informação e tecnologia



Fonte: elaborado pelas autoras (2024).

Conforme observado na Figura 4, a ocorrência das palavras documentos, segurança e sistemas estão no mesmo patamar e próximas aos contextos em que a informação é explorada, seguida da gestão. Identificou-se que, no conteúdo dos textos, os autores discutem que, na era da virtualidade, a informação assume a configuração de um ativo informacional estratégico, cujo valor é amplamente debatido como o principal recurso em qualquer setor da economia.

Nas discussões sobre o valor da informação, Valentim (2008), alinhada com as pesquisas de Teixeira e Valentim (2015), apresentou estudos que corroboram a relevância da informação na gestão estratégica e na tomada de decisões, ganhando relevância por meio do sujeito cognoscente. Além disso, é importante ressaltar que o valor da informação está intrinsecamente ligado à produção de produtos e serviços, uma consequência direta da globalização e da interconectividade em rede.

Os autores da vanguarda da CI têm se concentrado na interseção entre o valor da informação e sua aplicação na GI e na GC. Esses diálogos são cruciais para o desenvolvimento profissional dos especialistas em informação e são especialmente relevantes na era da informação digital.

Valentim (2008) e Santos e Valentim (2020) exploram a relação entre o valor da informação, a GC e a GI. Por outro lado, Silva (2017) também contribui para essa discussão, enfatizando a necessidade de uma ligação mais robusta entre os valores atribuídos, a informação pelos aspectos consequenciais, ligados a organizações e valores causais, especialmente aos sociais e humanos. Esse ponto de vista representa uma direção importante na CI.

Autores clássicos como Davenport e Prusak (1999), Urdaneta (1992) e Moresi (2000) destacam a relação entre dados, informação e conhecimento. No entanto, essa área continua a demandar uma análise constante, especialmente no sentido da informação em rede. Isso se deve à crescente interação entre a CI e a Ciência dos Dados, em que essas disciplinas se cruzam nos processos de acesso, tratamento, recuperação, compartilhamento e disseminação da informação.

Esse entrelaçamento assume especial importância no desenvolvimento da seção 3, em que se explorou o Sigad. A literatura investigada destacou o Sigad e sua relevância para o gerenciamento da informação e o ciclo de produção da informação no fluxo de trabalho. Isso ressalta que, na sociedade atual, é imperativo que as organizações implementem a GI em sistemas informatizados, uma evolução tecnológica irreversível, a fim de garantir sua sobrevivência e competitividade na Sociedade da Informação.

Foi observada uma tendência marcante em priorizar a exploração de normas e requisitos em relação às estratégias de segurança da informação em sistemas, considerando-os como entidades mecânicas. No entanto, embora seja crucial que os requisitos visem garantir o

funcionamento adequado desses sistemas, é igualmente essencial realizar uma análise das vulnerabilidades resultantes da interação dos usuários com esses sistemas.

Percebeu-se a ausência de pesquisas em que o usuário desempenhasse um posicionamento altivo como sujeito ativo no processo de segurança da informação. Mesmo a CTDE do Conarq concentra-se principalmente nos requisitos de proteção e invasão dos sistemas de informação, deixando em segundo plano o protagonismo do usuário.

As principais definições de segurança da informação, defendidas por Dhilon (2004), Sêmola (2003), Pimenta e Quaresma (2016) e outros autores destacados no corpus da pesquisa, concentram-se em questões éticas e na necessidade de conscientização acerca das boas práticas de segurança da informação.

A frequência das variáveis presentes na segurança da informação aponta que determinantemente a informação está associada aos processos de gestão organizacional e constituição do conhecimento, enquanto a ocorrência dos termos voltados para documentos e sistemas ficam mais próximos dos diálogos em que incluem os usuários e suas fragilidades como usuários dos sistemas informatizados.

A responsabilidade dos gestores na promoção de uma cultura de segurança da informação vai além da implementação de medidas técnicas. A literatura enfatiza a necessidade de abordar a dimensão ética, conscientizando os usuários sobre as implicações de suas ações e a importância de agir de forma responsável.

5. Considerações finais

A pesquisa possibilitou um explorar na literatura relacionada à segurança da informação, permitindo a identificação das principais perspectivas teóricas sobre o comportamento dos usuários em Sigad na interface entre homem, tecnologia e sistemas.

A análise da revisão bibliográfica destacou como esse tema tem sido explorado de maneira interdisciplinar, o que é uma característica dos estudos que têm a informação como seu foco central. Observou-se uma maior incidência na área da Ciência da Informação (CI), com correlações entre essa área e a Ciência dos Dados e a Ciência da Computação. Os aspectos socioculturais também ganharam relevância, incluindo abordagens voltadas para o estudo dos usuários e suas interações com o homem, a tecnologia e os sistemas.

Em termos práticos, observou-se que, com as funcionalidades dos Sigad, as organizações estão cada vez mais inclinadas a lidar com documentos produzidos eletronicamente. No entanto, ainda há casos em que alguns documentos são originados em formato físico e posteriormente convertidos para formatos digitais. Acredita-se que essa tendência levará, gradualmente, à eliminação dos procedimentos envolvendo documentos físicos.

Identificou-se uma convergência de ideias entre os autores discutidos nesta revisão, indicando que as organizações devem alinhar suas práticas de gestão documental com as melhores práticas de segurança da informação. Em resumo, a segurança da informação vai além da tecnologia e depende da conscientização e comprometimento das pessoas envolvidas. Ignorar essas dinâmicas comportamentais pode comprometer a segurança dos sistemas. Portanto, é crucial considerar a interação entre humanos e tecnologia na estratégia de segurança, garantindo o engajamento de todos na proteção de dados e sistemas.

Concluiu-se que as pesquisas precisam avançar e expandir, principalmente por meio de estudos de caso, intervenções e pesquisa-ação que possam instigar de maneira prática percepções e ações direcionadas a resguardar os Sigad das vulnerabilidades e riscos. Esses esforços não devem se restringir apenas às questões tecnológicas, mas também devem ser solidamente fundamentados nos pilares da segurança da informação e nas melhores práticas de segurança, especialmente nas interfaces entre usuários e sistemas.

Esta pesquisa não teve a pretensão de esgotar todas as possibilidades ou encerrar os debates sobre o tema. Acredita-se que sua principal contribuição tenha sido expandir o pensamento crítico para explorar novos horizontes do conhecimento no âmbito da CI e suas interconexões, com foco na segurança da informação como um processo amplo, com diferentes eixos investigativos.

Referências

ALENCAR, Thayane; ARAÚJO JÚNIOR, Rogério Henrique de. Os estudos das necessidades informacionais dos usuários de sistemas informatizados de gestão arquivística de documentos como subsídio para o planejamento estratégico. **Ágora**, Florianópolis, v. 32, n. 64, 2022. Disponível em: https://brapci.inf.br/index.php/res/v/169712. Acesso em: 11 set. 2023.

ALMEIDA, Maria Fabiana Izídro de; BIAGGI, Camila de; VITORIANO, Marcia Cristina de Carvalho Pazin. Identificação dos fluxos informacionais: contribuições para a gestão do conhecimento. **Ágora**, Florianópolis, v. 31, n. 63, p. 1–11, 2021. Disponível em: https://agora.emnuvens.com.br/ra/article/view/994. Acesso em: 20 jul. 2023.

ANDRADE, Denise; VALENTIM, Marta Lígia Pomim. Fluxo informacional: uma análise a partir do portal da secretaria de administração penitenciária. *In*: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 20, 2019, Florianópolis. **Anais** […]. Florianópolis: UFSC, 2019. Disponível em: https://brapci.inf.br/index.php/res/download/161938. Acesso em: 20 jun. 2023.

BARDIN, Laurence. **Análise de conteúdo**. 3. reimp. rev. ampl. São Paulo: Edições 70, 2011.

CASTELLS, Manuel. **A sociedade em rede**. 24. ed. São Paulo: Paz & Terra, 2013. 630 p.

CHOO, Chun Wei. **A organização do conhecimento**: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. Tradução de Eliana Rocha. São Paulo: Senac, 2003.

CONSELHO NACIONAL DE ARQUIVOS. Câmara Técnica de Documentos Eletrônicos. **Modelo de requisitos para sistemas informatizados de gestão arquivística de documentos**: e-ARQ Brasil. 2020. Disponível em: https://www.gov.br/conarq/pt-br/centrais-de-conteudo/publicacoes/EARQV203MAI2022.pdf. Acesso em: 12 jun. 2023.

COSTA, Eliandro dos Santos. **A descrição arquivística e a recuperação da informação na proposta de um modelo conceitual de sistemas informatizados de gestão arquivística de documentos:** um estudo em instituições de ensino superior. 2018. 160 f. Tese (Doutorado em Ciência da Informação) – Universidade Estadual Paulista, Unesp, Marília, SP, 2018. Disponível em: https://repositorio.unesp.br/handle/11449/153808. Acesso em: 20 ago. 2023.

DAVENPORT, Thomas; PRUSAK, Laurence. **Conhecimento empresarial**. Tradução de Lenke Peres. Rio de Janeiro: Campus: São Paulo: Publifolha, 1999. 237 p.

DHILLON, Gurpreet. Realizing benefits on an information security program. **Business Process Management Journal**, Texas, v. 10, n. 3, p. 260-261, 2004. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/bpmj.2004.15710caa.002/full/html. Acesso em: 20 abr. 2020.

FERREIRA, Sérgio da Costa. **Sistemas de informação em segurança**. Londrina: Editora e Distribuidora Educacional, 2017. 224 p.

FURNELL, Steven; THOMSON, Kerry-Lynn. From culture to disobedience: recognizing the varying user acceptance of IT security. **Computer Fraud & Security**, Amsterdam, NL, 2. ed., v. 2009, n. 2, p. 5-10, fev. 2009. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1361372309700193. Acesso em: 12 maio 2023.

HITCHINGS, Jean. Deficiencies of the traditional approach to information security and the requirements for a new methodology. **Computers & Security**, Amsterdam, v. 14, n. 5, p. 377–383, May 1995. Disponível em: https://www.sciencedirect.com/science/article/pii/016740489597088R. Acesso em: 20 ago. 2022.

JADERTRIERVEILER, Heron; SELL, Denilson; SANTOS, Neri dos. The benefits and challenges of digital transformation in Industry 4.0. **Global. Journal of Management and Business Research**: a administration and management, Massachusetts, v. 19, n. 12, p. 17-40, jan. 2019. Disponível em: https://journalofbusiness.org/index.php/GJMBR/article/view/2926/2827. Acesso em: 30 maio 2023.

MARCIANO, João Luiz Pereira. **Segurança da informação**: uma abordagem social. 2006. 212 f. Tese (Doutorado em Ciência da Informação) – Departamento de Ciência da Informação e Documentação, Universidade de Brasília, Brasília, 2006. Disponível em: https://repositorio.unb.br/handle/10482/1943. Acesso em: 12 ago. 2022.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos da metodologia científica**. 8. ed. São Paulo: Atlas, 2017. 372 p.

MORESI, Eduardo Amadeu Dutra. Delineando o valor do sistema de informação em uma organização. **Ciência da Informação**, Brasília, v. 29, n. 1, p. 14-24, jan./abr. 2000. Disponível em: https://revista.ibict.br/ciinf/article/view/895/932. Acesso em: 20 abr. 2023.

PIMENTA, Alexandre Manuel Santanero; QUARESMA, Rui Filipe Cerqueira. A segurança dos sistemas de informação e o comportamento dos usuários. **Revista de Gestão da Tecnologia e Sistemas de Informação**, São Paulo, v. 13, n. 3, p. 533-552, set/dez. 2016. Disponível em: https://www.scielo.br/j/jistm/a/n6HBtP6htxYkTKKrjt9VsRz/?format=pdf. Acesso em: 15 abr. 2023.

SANTOS, Henrique Machado dos; FLORES, Daniel. Novos rumos da preservação digital: das estratégias aos sistemas informatizados. **Biblios**: Revista de Bibliotecología y Ciencias de la Información, Peru, PE, n. 70, p. 31-43, 2018. Disponível em: https://brapci.inf.br/index.php/res/download/168300. Acesso em: 20 ago. 2023.

SANTOS, Juliana Cardoso dos Santos; VALENTIM, Marta Lígia Pomim. Informação, conhecimento e valor da informação. **Informação e Informação**, Londrina, v. 25, n. 4, p. 574 – 598, out./dez. 2020. Disponível em: https://ojs.uel.br/revistas/uel/index.php/informacao/article/view/39991. Acesso em: 12 abr. 2023.

SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2003.

SILVA, Jonathas Luiz Carvalho. Informação e valor: inter-relações conceituais e a formação das tipologias valorativas da informação. **Transinformação**, Campinas, v. 29, n. 3, set./dez. 2017. Disponível em: https://www.scielo.br/j/tinf/a/B7RSLGJvC5mSzTtJybJgxvP/abstract/?lang=pt. Acesso em: 20 ago. 2022.

SILVA, Margareth da; ROCHA, Cláudia Lacombe. A revisão dos requisitos e metadados do e-ARQ Brasil versão 2.0. **Officina**: Revista da Associação de Arquivistas de São Paulo, São Paulo, v. 1, n. 2, p. 09-26, 2022. Disponível em: https://brapci.inf.br/index.php/res/download/213649. Acesso em: 15 jul. 2023.

TEIXEIRA, Thiciane Mary Carvalho; VALENTIM, Marta Lígia Pomim. Inteligência competitiva organizaiconal. **Tendências da Pesquisa Brasileira em Ciência da Informação**, João Pessoa, v. 8, n. 2, 2015. Disponível em: https://brapci.inf.br/index.php/res/v/151647. Acesso em: 12 maio 2023.

URDANETA, Iraset Páez. **Gestión de la inteligencia, aprendizaje tecnológico y modernización del trabajo informacional**: retos y oportunidades. Caracas: Instituto de Estudios del Conocimiento de la Universidad Simón Bolivar, 1992. 253 p.

VALENTIM, Marta Lígia Pomim. Informação e conhecimento em organizações complexas. *In*: VALENTIM, Marta (org.). **Gestão da informação e do conhecimento**. São Paulo: Polis: Cultura Acadêmica, 2008. p. 11-25.

VENDRAMINI, Virgínia; ALEIXO, Diana Vilas Boas Souto. A gestão de documentos frente aos requisitos SIGAD. **Informações@profissões**, Londrina, v. 10, n. 1, p. 142-162, jan./abr. 2021. Disponível em: https://ojs.uel.br/revistas/uel/index.php/infoprof/article/view/43395/pdf_1. Acesso em: 12 ago. 2023.

Artigo submetido em: 17 out. 2023
Artigo aceito em: 21 ago. 2024